Cybersecurity Threats

No: 19
Jasmin

No: 20
Kaleb

No: 21
Kalid

No: 22
Keneni

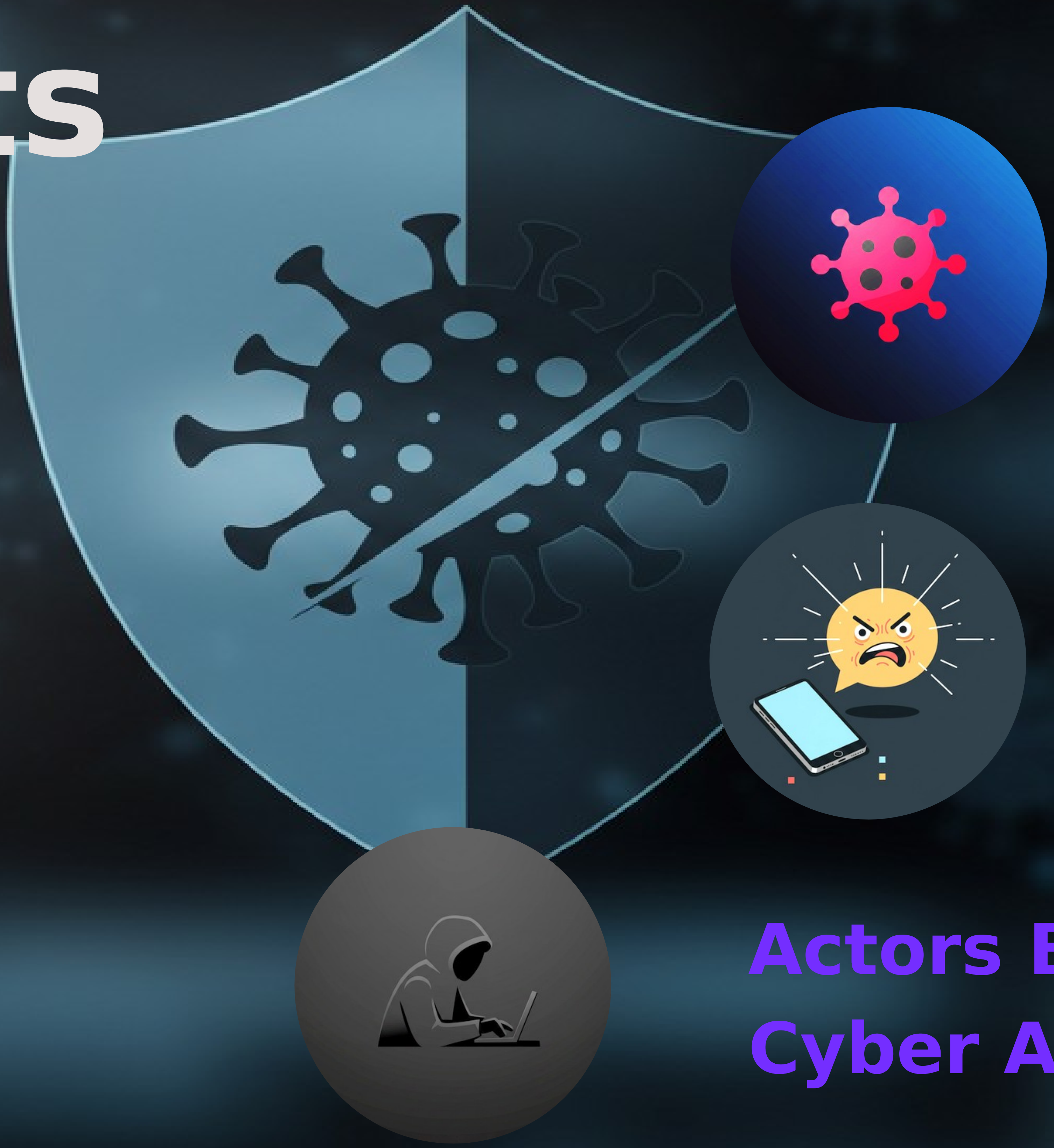
No: 23
Kidus

No: 24
Kiya

No: 25
Mahider

No: 26
Merjan

No: 27
Natinael



Types of Cyber Attacks

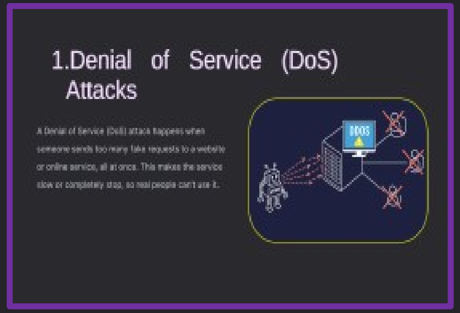
Online Challenges for Kids and Youth

Actors Behind Cyber Attacks

Types of Cyber Attack

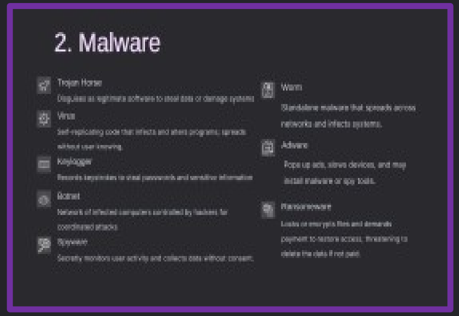
- A cyber attack is a harmful action using computers or the internet.
- The goal is to steal data, damage systems, or cause disruption.
- It can target individuals, companies, or governments. Common types include:

1. Denial of Service (DoS)
2. Malware
3. Man-in-the-Middle
4. Phishing
5. Eavesdropping
6. SQL Injection
7. Password Attack
8. Social Engineering



1.Denial of Service (DoS) Attacks

A Denial of Service (DoS) attack happens when someone sends too many fake requests to a website or online service, all at once. This makes the service slow or completely stop, so real people can't use it.



2. Malware

Trojan Horse
Disguises as legitimate software to steal data or damage systems

Virus
Self-replicating code that infects and alters programs; spreads without user knowing.

Keylogger
Records keystrokes to steal passwords and sensitive information

Botnet
Network of infected computers controlled by hackers for coordinated attacks

Spyware
Secretly monitors user activity and collects data without consent.

Worm
Standalone malware that spreads across networks and infects systems.

Adware
Pops up ads, slows devices, and may install malware or spy tools.

Ransomeware
Locks or encrypts files and demands payment to restore access, threatening to delete the data if not paid.

3. Man-in-the-Middle (MitM) Attacks

This type of attack includes intercepting communication between the people and then stealing data from their conversation. Open Wi-Fi networks are the most common place where this kind of attack takes place.

4. Phishing Attack

Phishing attacks are fake messages (usually emails) that look like they're from a trusted source. The goal is to trick people into giving away personal information like passwords or credit card details, or to get them to click links that install harmful software. It's a common cyber-attack, so everyone should know how to spot and avoid it.

8. Social Engineering Threats

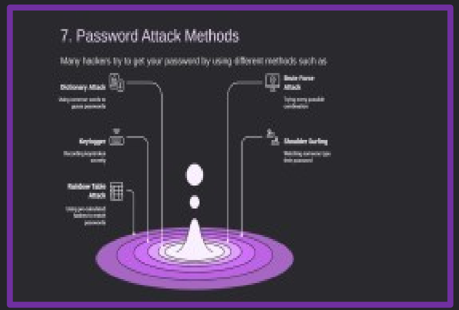
Social engineering refers to creating a social situation to get information from the user. This is often achieved through tactics such as

Impersonation
Attackers pose as trusted entities like service providers or colleagues.

Urgency Creation
Creates false time pressure to force hasty decisions.

Trust Exploitation
Manipulates human psychology to extract confidential information.

Social engineering bypasses technical safeguards by targeting the human element.



7. Password Attack Methods

Many hackers try to get your password by using different methods such as

5. Eavesdropping

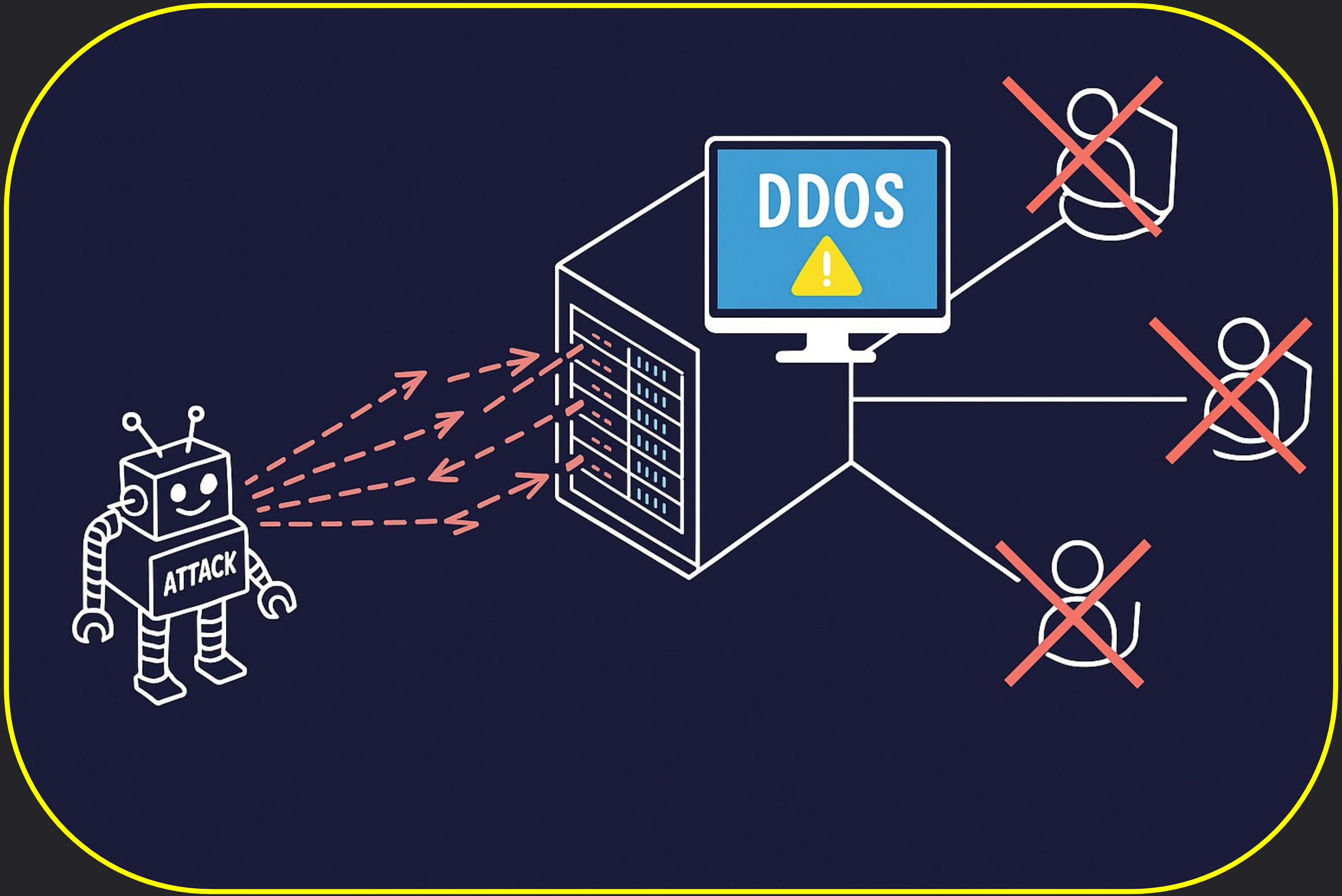
Eavesdroppers secretly listen to private conversations to steal information like passwords or credit card numbers. For example, a hacker might grab personal details from someone using an unprotected Wi-Fi network.

6. SQL Injection

SQL injection is when a hacker uses harmful SQL code in a website's form to steal or change data, like passwords. If the website doesn't check the input, the hacker can access sensitive information.

1. Denial of Service (DoS) Attacks

A Denial of Service (DoS) attack happens when someone sends too many fake requests to a website or online service, all at once. This makes the service slow or completely stop, so real people can’t use it.



2. Malware

Trojan Horse

Disguises as legitimate software to steal data or damage systems

Virus

Self-replicating code that infects and alters programs; spreads without user knowing.

Keylogger

Records keystrokes to steal passwords and sensitive information

Botnet

Network of infected computers controlled by hackers for coordinated attacks

Spyware

Secretly monitors user activity and collects data without consent.

Worm

Standalone malware that spreads across networks and infects systems.

Adware

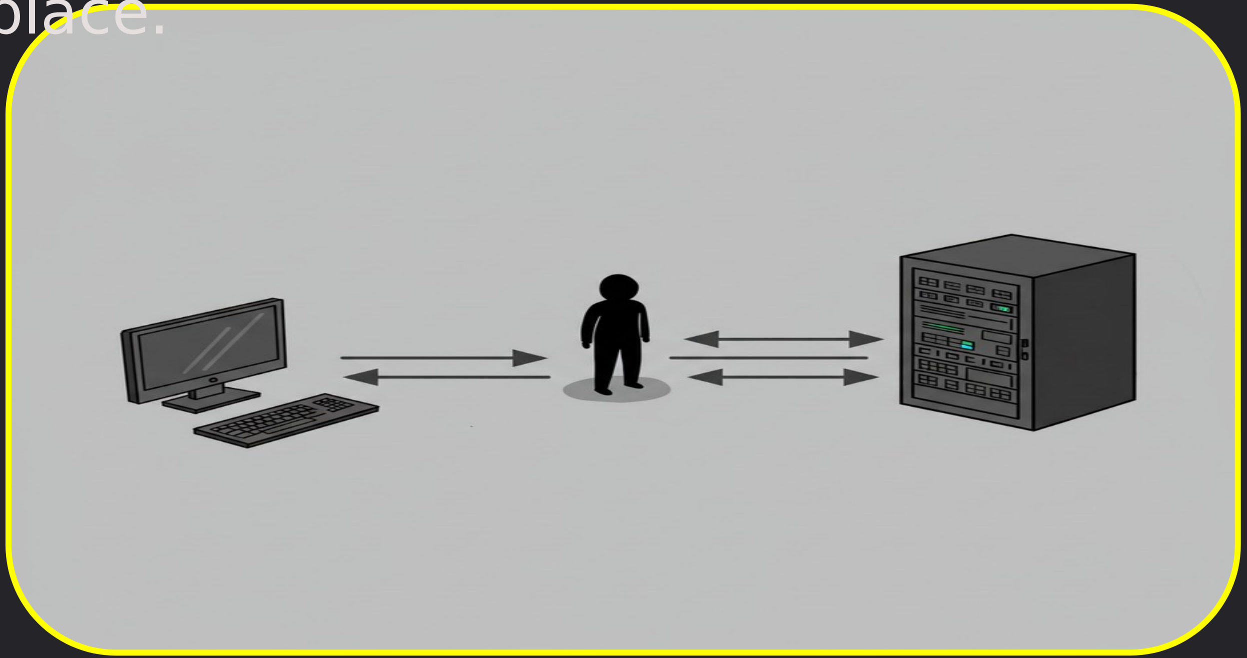
Pops up ads, slows devices, and may install malware or spy tools.

Ransomeware

Locks or encrypts files and demands payment to restore access, threatening to delete the data if not paid.

3. Man-in-the-Middle (MitM) Attacks

This type of attack includes intercepting communication between the people and then stealing data from their conversation. Open Wi-Fi networks are the most common place where this kind of attack takes place.

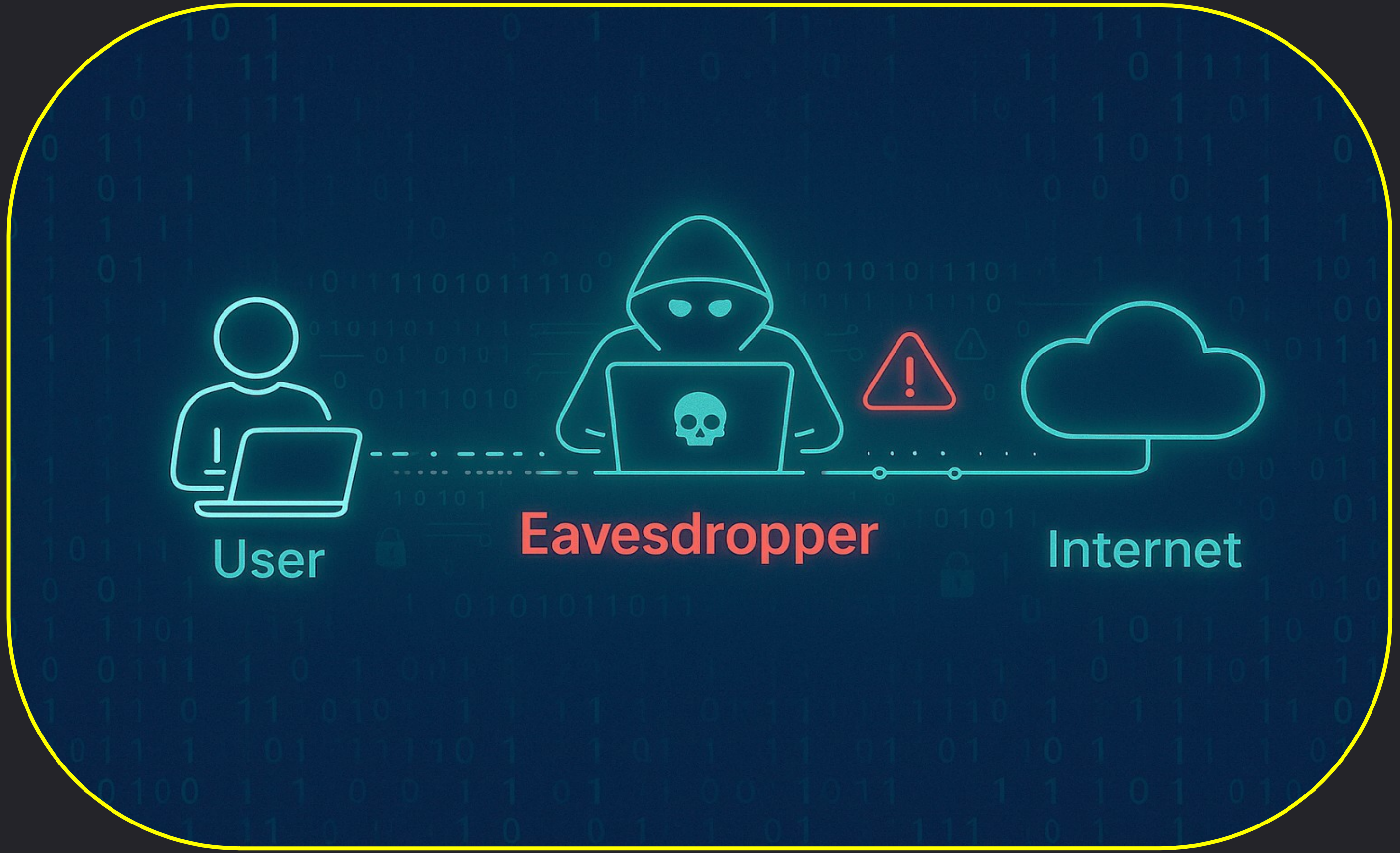


4. Phishing Attack

Phishing attacks are fake messages (usually emails) that look like they’re from a trusted source. The goal is to trick people into giving away personal information like passwords or credit card details, or to get them to click links that install harmful software. It's a common cyber-attack, so everyone should know how to spot and avoid it.

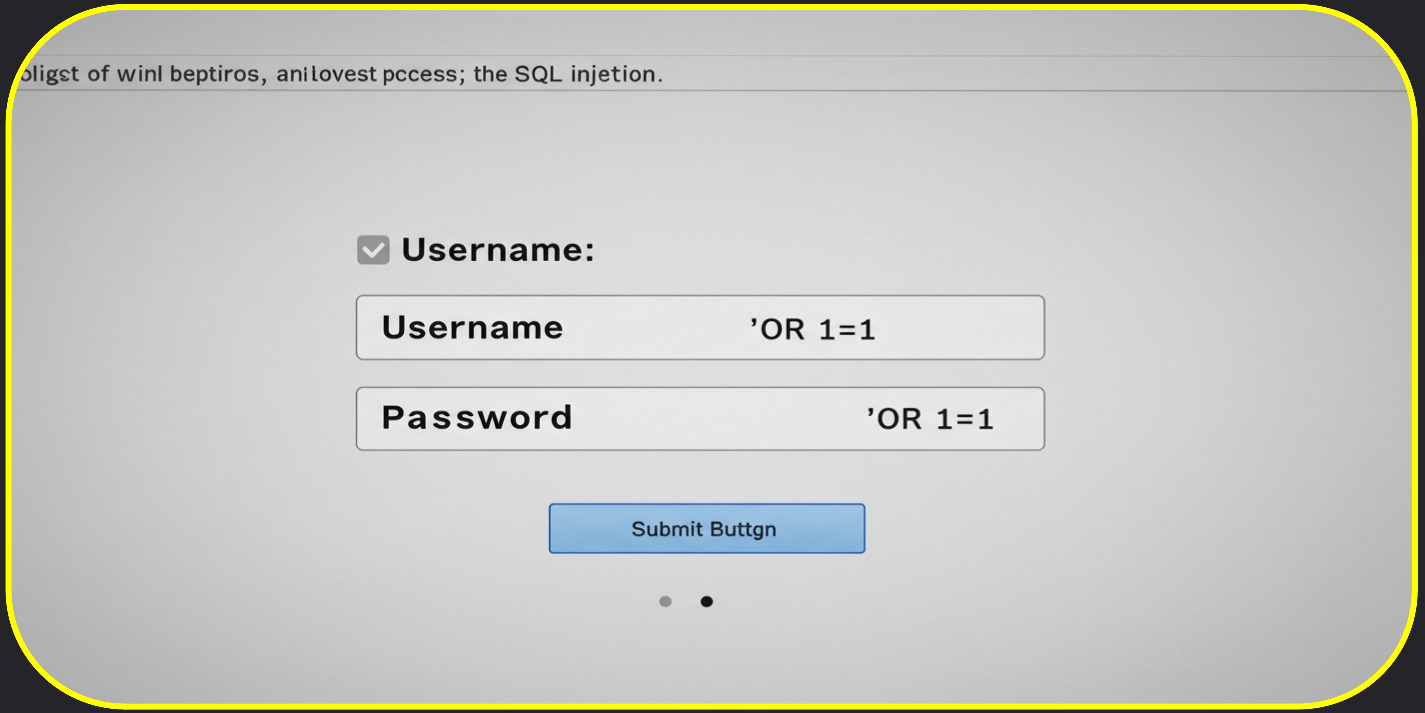
5. Eavesdropping

Eavesdroppers secretly listen to private conversations to steal information like passwords or credit card numbers. For example, a hacker might grab personal details from someone using an unprotected Wi-Fi network.



6. SQL Injection

SQL injection is when a hacker uses harmful SQL code in a website’s form to steal or change data, like passwords. If the website doesn’t check the input, the hacker can access sensitive information.



oligst of winl beptiros, anilovest pccess; the SQL injetion.

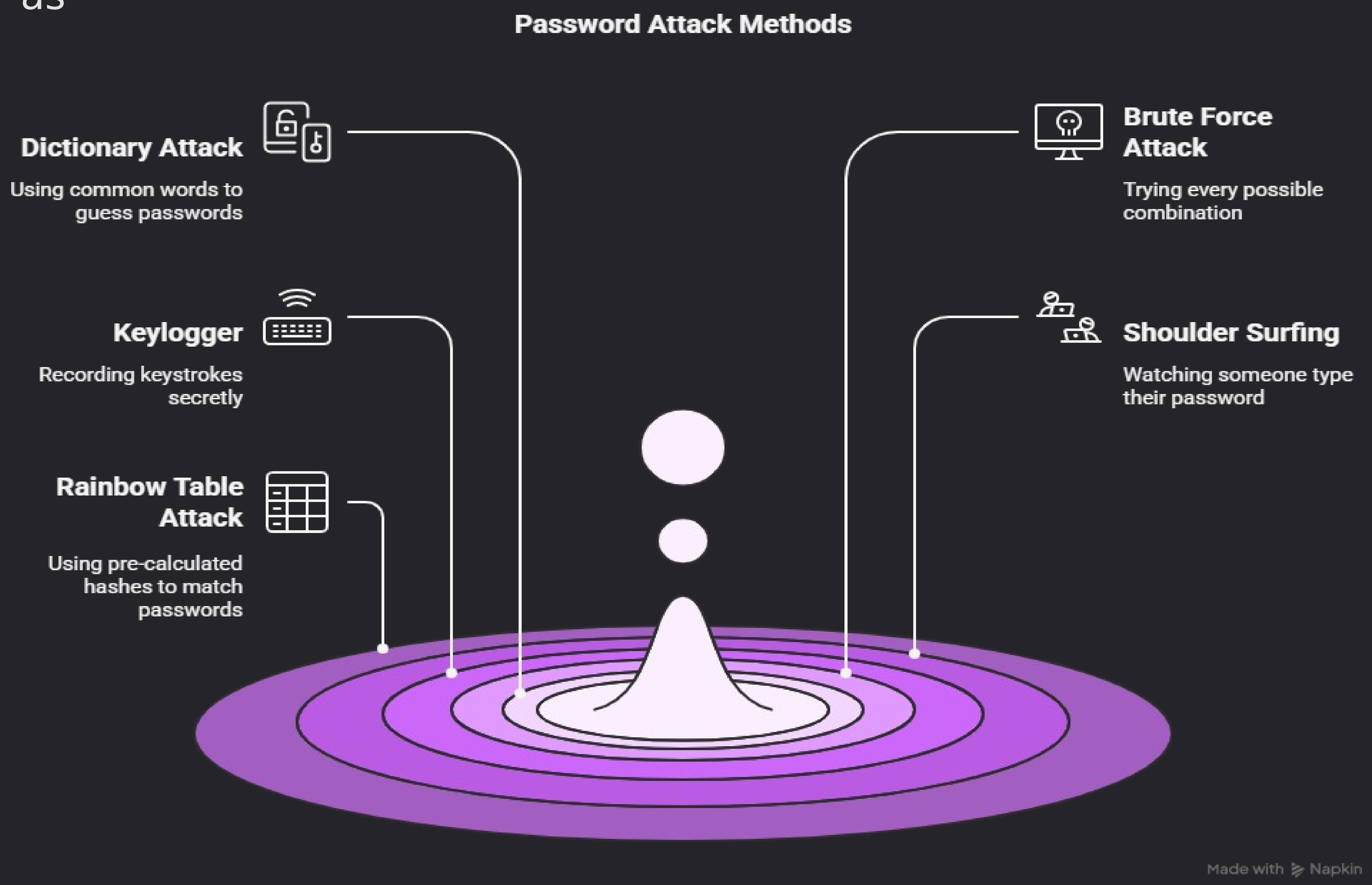
☑ Username:

Username ’OR 1=1

Password ’OR 1=1

7. Password Attack Methods

Many hackers try to get your password by using different methods such as



Password Attack Methods

Dictionary Attack

Using common words to guess passwords

Keylogger

Recording keystrokes secretly

Rainbow Table Attack

Using pre-calculated hashes to match passwords

Brute Force Attack

Trying every possible combination

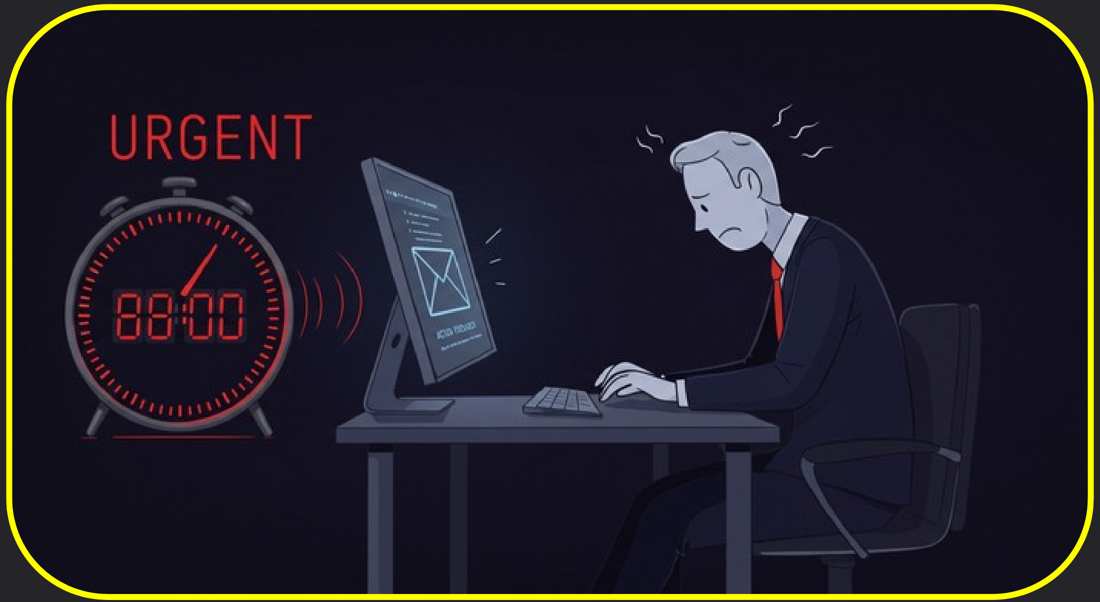
Shoulder Surfing

Watching someone type their password

Made with Napkin

8. Social Engineering Threats

Social engineering refers to creating a social situation to get information from the user. This is often achieved through tactics such as



Impersonation

Attackers pose as trusted entities like service providers or colleagues.

Urgency Creation

Creates false time pressure to force hasty decisions.

Trust Exploitation

Manipulates human psychology to extract confidential information.

Social engineering bypasses technical safeguards by targeting the human element.

Online Challenges for Kids and Youth

The Internet is risky for kids and youth, with extremists, terrorists, and traffickers using it to harm them. These online dangers threaten safe browsing.

Cyberbullying

Persistent online harassment involving false, harmful, or embarrassing content via social media, messaging apps, or games, often causing severe psychological effects.

Cyber Predators

Adults exploit online anonymity to target minors for exploitation. Predators use grooming techniques, misrepresenting their identity and establishing trust before initiating harmful contact.

Privacy Vulnerability

Young users share personal information online, including details like addresses, school locations, and routines, creating safety and privacy risks without understanding consequences.

Threat Actors

Hackers

Technical specialists with varying motivations, from testing security boundaries to causing disruption without specific targets

Online Criminals

Professional cybercriminals specifically targeting valuable data for financial gain through theft or ransomware operations

Malicious Insiders

Organizational members exploiting legitimate access to compromise systems or exfiltrate sensitive information

School Pupils

Young individuals testing technical skills without fully understanding potential legal and ethical consequences

Honest Mistake

Sometimes persons like you or staff with the best intentions just make a mistake, for example by emailing something sensitive to the wrong email address.